Service Definition: Desktop as a Service

Crown Commercial Services | G Cloud 15 framework

Contents

Document Information

Client name	G Cloud 15 Service Definition
Project name	Desktop as a Service
Document author(s)	Lee Gothard, Gill Brown

Document Change Record

Issue	Date	Description
V0.1	01/12/25	Draft Template
V0.2	12/12/25	Draft Initial Content added
V0.3	22/01/26	Draft for review and sign off
V1.0	27/01/26	Final for issue

Contact Information

This document has been supplied by Roc Technologies Limited, whose registered office is:	Roc Technologies Limited 1 Lindenmuth Way Greenham Business Park Greenham Thatcham RG19 6AD United Kingdom
Please refer all enquiries to:	**Gill Brown, 0845 647 6000** publicsector@roctechnologies.com.

Confidentiality Agreement

All information contained in this document, including any prices quoted, is to be treated as confidential. It shall not be used for any other purpose and shall not be published or disclosed wholly or in part to any other party without the express written permission of Roc Technologies Limited and shall be held in safe custody.

These obligations shall not apply to information that is in the public domain or becomes known legitimately from some source other than Roc Technologies Limited. All intellectual property rights of products or services provided by Roc Technologies Limited shall remain vested in Roc Technologies Limited.

Non-Disclosure

None of the information may be used by the client for any other purpose, nor may it be disclosed by them otherwise than, firstly to members of its staff who will be engaged in the evaluation and, secondly, to representatives of any organisation acting in the capacity of professional adviser to the client. Before making this document available for evaluation, the client must bring this notice to the attention of those concerned.

Proprietary Information

The information in this document has been reviewed and is believed to be accurate. However, neither Roc Technologies Limited. nor its affiliates assume any responsibility for inaccuracies, errors, or omissions that may be contained herein. In no event will Roc Technologies Limited or its affiliates be liable for direct, indirect, special, incidental, or consequential damages resulting from any defect or omission in this document, even if advised of the possibility of such damages.

Roc Technologies Limited reserves the right to make improvements or changes to this document and information contained within, and to the products and services described at any time, without notice or obligation.
Roc Technologies understands that any award to supply the products and/or provide the services that are the subject of this document is subject to the mutual execution of a definitive written agreement.
All information supplied for the purpose of this Roc Technologies document is to be considered confidential.

1. Service Summary

As a solutions aggregator and specialist managed services provider, Roc Technologies (Roc) have been implementing and supporting IT Solutions for over twenty years. We maintain, transform, and manage IT systems that enable organisations to grow and flourish. Whatever the requirement, Roc can manage all your hardware and software needs, from servers and desktops to applications, data, and networks. We support our customers throughout the IT lifecycle, from initial strategy development and technology assessment - through to innovative design and procurement processes, implementation, and management.

Roc is well versed in providing managed desktops for users. This is built on its core skills in Citrix and Microsoft technologies. This is not just providing a solution and service for managing a customers' desktop on their infrastructure/Cloud but also providing a desktop on a price per user basis.

In addition to Microsoft and Citrix technologies, we also have expertise in complimentary services such as Nerdio.

Nerdio can provide significant value add for customers when deploying virtual desktop environments.

Roc has a long-standing partnership with both Microsoft and Citrix and have been the enabler for transition of Citrix workloads to Microsoft Azure Virtual Desktop, through our experience and thorough understanding of the Citrix and AVD product capabilities.

To summarise Roc's Desktop as a service capability:

- Based on 20 years of experience with Citrix & Microsoft.
- Combining the strengths of Citrix Desktop as a service & Microsoft Azure, including Azure Local and Windows 365.
- Designed for secure & sensitive organisations.
- Optimised to support Unfired Comms & Collaboration.
- Packaged deployment, migration and operations services.
- Use cases include:
    - Delivering a consistent, device agnostic experience.
    - Sweating investment on existing end-user devices.
    - Securing sensitive data.
    - Transformation/migration solution.
    - Cloud Cost Optimisation.
    - Proactive Cloud advice.
    - Business value and outcomes based, delivering Cloud success.

2. Service Description

Roc's Desktop as a service is based on the deployment of either Windows 365 cloud PC, Azure Virtual Desktop or AVD with Azure Local, which can be integrated with Nerdio Manager for Enterprise and is designed to support on-premises, public cloud, hybrid and private cloud infrastructure environments. Roc are partners with Microsoft, with Gold and Silver partnerships with Citrix and Nerdio respectively.

The information below provides information on Citrix and Windows Virtual desktop. Roc also provides service for managing traditional desktops. These can be summarised as follows:

1. Patching services for end user desktops
2. Asset and monitoring services for end user desktops
3. Site visits and auditing services to provide user support and back-end infrastructure teams with quality data
4. Desk side support utilising Roc's field services teams

Items 1 and 2 may require an agent to be deployed to the user's devices, dependent on any management system in use.

2.1. Using Azure Virtual Desktop

Virtual desktop infrastructure is a desktop virtualisation technology wherein a desktop operating system, typically Microsoft Windows, runs and is managed in a data centre. Azure Virtual Desktop (AVD) is Microsoft's proprietary desktop and app virtualisation service that runs in the Azure Cloud or in a hybrid scenario through Azure Local deployments.

Roc has proven experience of working with clients to deliver Microsoft Virtual desktop services. These can be delivered either via Windows 365 cloud PC for small deployments or Azure virtual desktop (AVD) for larger engagements.

Roc would work with the client to deploy master images utilising Windows 11 multi-session capabilities, integrating Azure Monitor and FSLogix. Microsoft recommends FSLogix profile containers as a user profile solution. FSLogix is designed to roam profiles in remote computing environments, such as AVD, storing a complete user profile in a single container.

Roc would also look to integrate the AVD environment with the existing Azure networking and identity management mechanisms. In addition, Roc can work with the client to integrate their conditional access and Azure Multi-Factor Authentication (MFA) services.

Listed below are the key pre-requisites for successful AVD deployment, Roc would look to address these requirements during initial testing, ideally using a Proof of Concept (POC stage).

Pre-requisites needed to deploy AVD:

- Azure Subscription – To deploy virtual machines, network resources, and all the items typically need to spin up a VM, including Desktop Virtualization resource provider for your subscription.
- Microsoft Entra ID (Formerly Azure AD) If you are already using O365, Intune, or other Microsoft cloud services, you already have this.
- An identity strategy e.g. Active Directory (AD), Microsoft Entra ID and Microsoft Entra ID connect.
- All associated Azure resources including image, virtual network, storage etc. hosted in one region.
- Appropriate Microsoft Licensing.

Roc would work with the client to identify licensing requirements and any shortfall.

Azure Virtual desktop provides three different virtual desktop options:

- **Pooled Multi-Session:** A set of VMs that are temporarily assigned to users as they sign in, based on the load-balancing algorithm of the broker. Every time a user signs in, the user may be assigned a different VM. Multiple users are connected to the same virtual machine simultaneously.
- **Pooled Single Session:** A set of VMs that are temporarily assigned to users as they sign in, based on the load-balancing algorithm of the broker. Every time a user signs in, the user may be assigned a different VM. Only one user is assigned per virtual machine.
- **Personal:** Personal is when a single user occupies a specific virtual machine and it is not shared with other users, similar to if a user had a dedicated physical PC.

There are different use cases for each of these options. Pooled muti-session VMs are suitable for groups of users that have a common list of applications and do not have any requirement to customise their desktop or to have administrative or update rights on the server. All users on a single VM share single instances of applications and other resources. This fits well with typical user personas. This model is most cost effective were large numbers of users with modest IT needs can share a single server. A defined baseline will reduce the number of users that can share a server or require more expensive high end virtual machines.

Pooled single session and personal desktops are more appropriate where the user requires a level of administrative access to the device for example to be able to do their own updates or install or remove software. They can also be appropriate where the number of users with similar requirements is relatively low limiting the efficiencies of scale that can be achieved with shared desktops.

2.2. Using Azure Virtual Desktop with Azure Local

Azure Virtual Desktop (AVD) deployed with Azure Local provides organisations with a secure, high-performance virtual desktop solution that runs on-premises while maintaining full integration with the Azure cloud. This hybrid approach enables businesses to deliver virtual desktops and applications close to their users for low-latency experiences, while leveraging

Azure's centralised management, security, and scalability. By combining Azure Local infrastructure with AVD, organisations can meet regulatory or data residency requirements, optimise performance for branch locations, and maintain consistent governance across both on-premises and cloud environments.

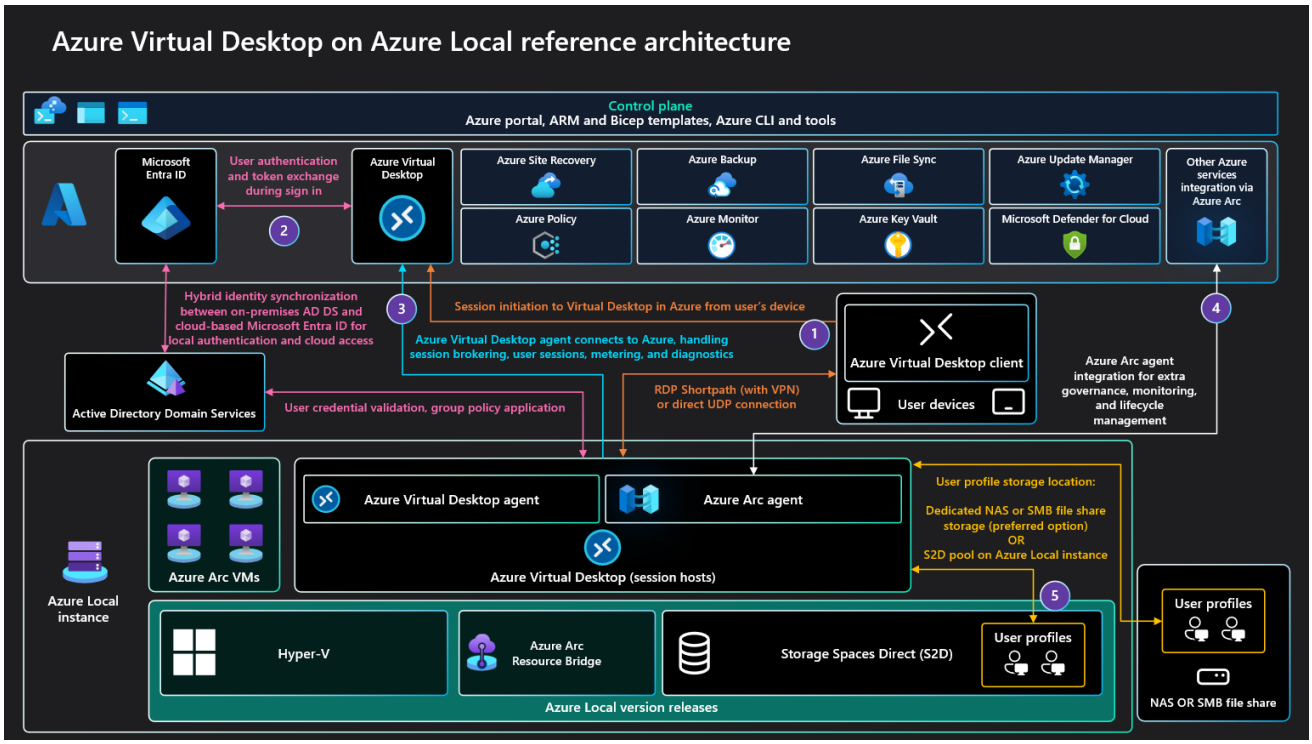

Figure 1 - Microsoft AVD / Azure Local reference architecture

2.3. Using Citrix Desktop

Roc maintains a long-standing partnership with Citrix and has extensive experience in designing, deploying, and managing Citrix environments for a wide range of customers. Through our managed service offering, we provide comprehensive support for Citrix platforms. Additionally, we assist organisations in transitioning from Citrix to Azure Virtual Desktop (AVD), leveraging our deep understanding of Citrix technologies and proven expertise in delivering successful AVD deployments.

2.4. Nerdio Manager

In the dynamic landscape of virtual desktop infrastructure (VDI), managing resources efficiently on platforms like Azure Virtual Desktop (AVD) can be a complex task. However, Nerdio offers a comprehensive solution to simplify the deployment, optimisation, and day-to-day management of AVD environments.

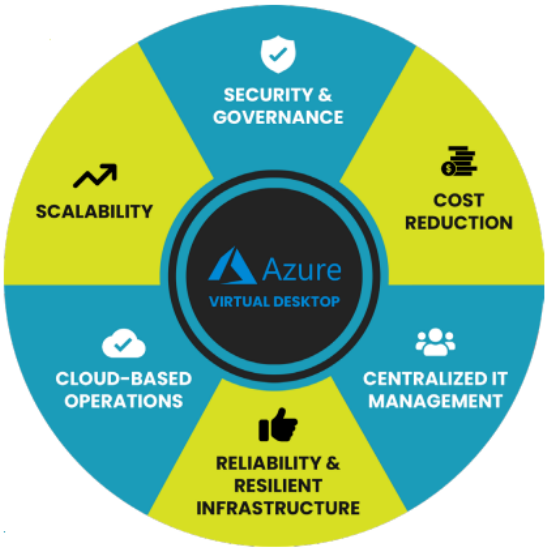

Figure 2 – Nerdio Management Capability

For this reason, Roc includes the option of deploying Nerdio for ongoing platform management as a costed option. Nerdio Manager for Enterprise allows customers to leverage the significant investments Microsoft is making into Azure Virtual Desktop, Intune, and Windows 365 services. Unlike other virtual desktop solutions, Nerdio Manager for Enterprise does not replace Microsoft's native components but enhances them with best-in-class enterprise capabilities and extends native admin experience.

Enterprise IT professionals can deliver and maintain a wide range of virtual Windows endpoints and Windows applications across hybrid workforces with ease and fine-tune end-user computing (EUC) approaches for maximum effectiveness using powerful monitoring and analytics capabilities.

In conclusion, Nerdio emerges as a comprehensive solution for organisations seeking to streamline and optimise their Azure Virtual Desktop management. As the technology landscape continues to evolve, Nerdio remains at the forefront, simplifying the complexities of VDI and empowering administrators to take control of their AVD environments. Nerdio Manager for Enterprise delivers over 200 additional features & benefits on top of the native AVD service. It allows IT admins and BAU teams to do the following actions with ease:

Simplify & Automate

- Deploy a complete AVD environment in two hours, from start to end-user login.
- Manage AVD, Windows 365, and MSIX AppAttach from a complete and powerful portal that is easy to use.
- Fully automate image creation, patching, and session host updates without advanced PowerShell scripting

Scale & Optimise

- Create dynamic host pools that shrink and expand in response to user demand and time of day.

- Save up to 75% on unoptimized Azure compute and storage consumption with sophisticated Auto-scaling.
- Optimise performance and costs by matching infrastructure size to user demand in real time, at any scale.

Secure & Protect

- Build resilient and highly available AVD and Windows 365 deployments with availability zones.
- Implement role-based, “least privilege” administration and enable end-user self-service.
- Maintain security compliance.

Integration with Intune

- Provides a single pane of glass for managing Azure Virtual Desktop (AVD), Windows 365, and Intune policies together.
- Simplifies administration by integrating Intune device and app management into the Nerdio dashboard.

2.5. Example Deployment

The diagram below illustrates a reference deployment of Microsoft AVD and Nerdio Manager, aligned to Roc best practice.

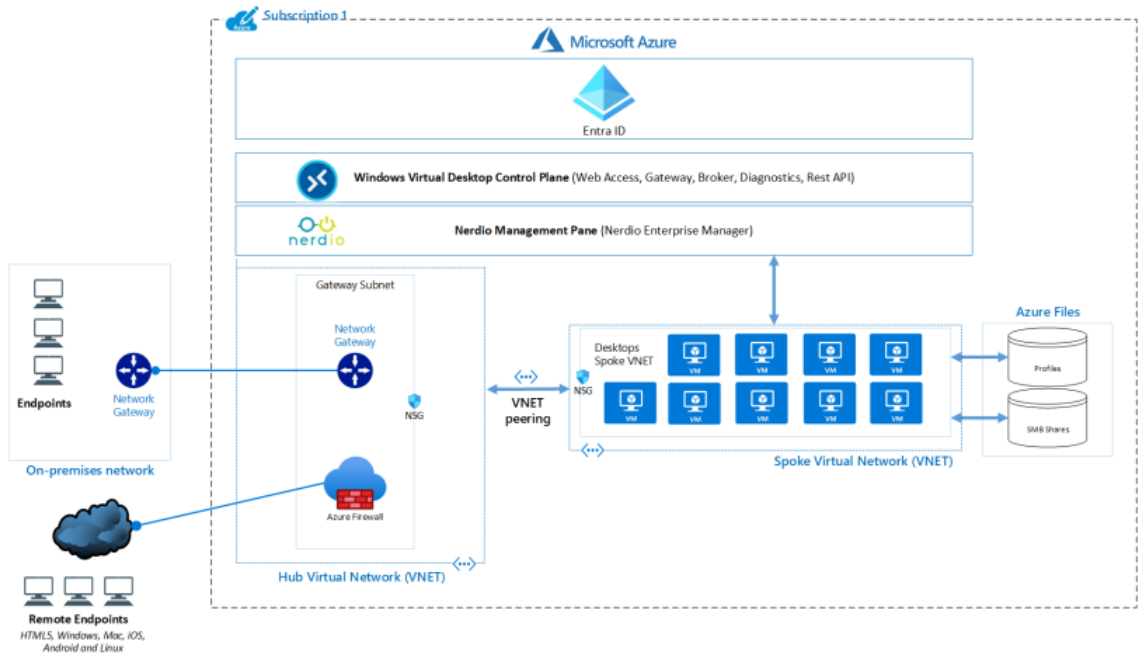

Figure 3 – Reference AVD & Nerdio Deployment

Roc deployed the following feature sets:

- Entra ID: Identity management platform in Azure for user login and permissions. Entra ID domain services will be used manage access rights to files and folders.

- Azure AVD: Virtual desktop hosting, one pool for each group and a mixture of shared and personal desktops
- Nerdio Enterprise Manager: Management pane for deployment, automation and scaling of the solution.
- Intune: To manage session hosts and security policies.
- VPN Gateway: To allow remote access to file storage for admin purposes.
- Firewall: To control traffic and out of Aure including VDI access to the internet.

2.6 Service Delivery

Roc offers packaged services for moving customers to a Cloud managed desktop, using the approach below:

Figure 4 – Roc Managed Desktop Methodology

2.7 Support Model

The services within this document are designed to operate as a first line service desk, second or third level resolver groups.

Additionally, where a separate 1st line desk is in use, Roc request that the clients service desk will operate during the same hours as the selected Roc service and manage communications amongst client stakeholders.

2.7.1 Accreditations & Vetting

Roc's Security services are delivered from Roc's UK based Technical Operation Centre (TOC) and a dedicated Security Operation Centre (SOC). All team members are DBS and BPSS checked and where required, Roc are also able to provide SC and DV cleared resources.

Services are delivered in alignment with ITIL and Cyber Essentials standards, as well as ISO 20000, ISO 27001, ISO 9001 and ISO 14001.

Roc's commitment to aligning with industry best practices and ensuring the highest standards of service management, information security, and cybersecurity are paramount in our approach to delivering services. We confirm our alignment with ITIL V4 principles, our ISO27001 accreditation, and our Cyber Essentials Plus certification, underscoring our provision of a secure, efficient, and customer-centric service delivery model.

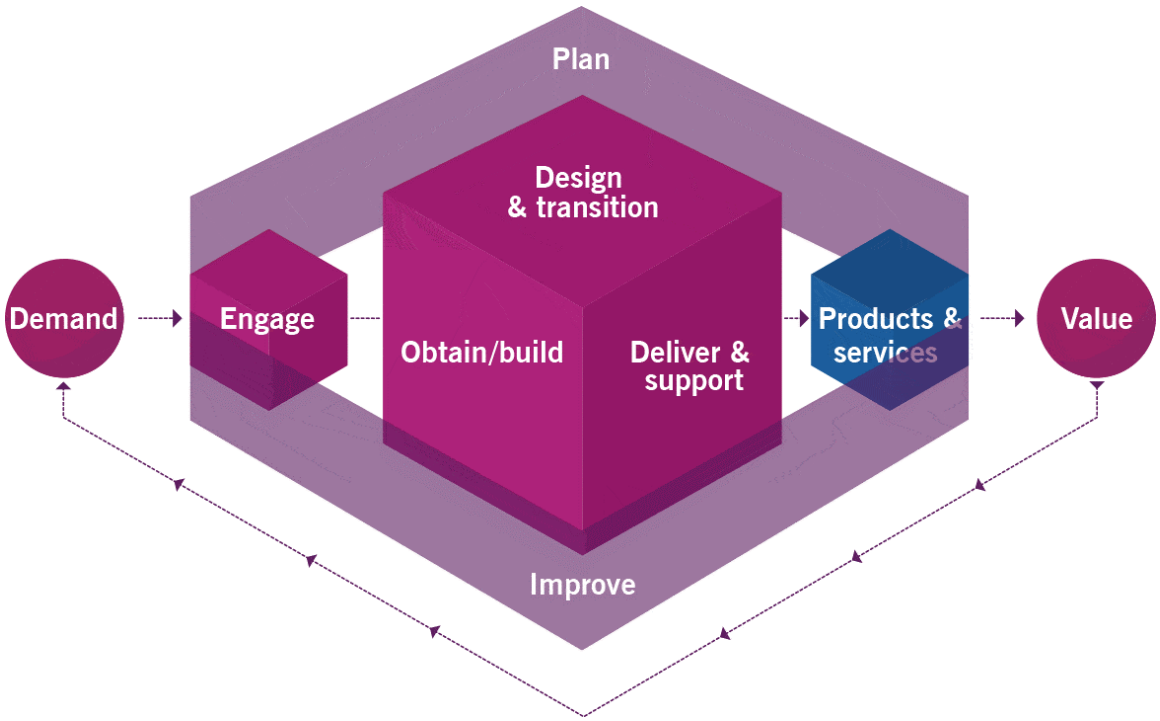

Figure 5 – ITIL Framework

Roc can offer Managed Services and Consultancy to prospective Clients. Roc considers security of our own and our customers' systems to be an imperative. We hold the ISO27001 standard for Information Security Management Systems (ISMS) and for some of our existing managed service customers we require the highest level of security accreditations to meet their security and controls, these include CESG (the UK Government's National Technical Authority for Information Assurance) and the National Cyber Security Centre (NCSC). Roc also provides managed services for several customers within secure and sensitive industries.

2.7.2 Support Mechanism

As a matter of routine, all services are delivered remotely. Roc assumes that an existing, industry standard remote access mechanisms will be available, via the internet, SD-WAN, PSN, N3, RLI or dedicated client WAN. Roc also offers a range of optional field engineering services where required to support hybrid cloud components such as network infrastructure or private cloud platforms.

2.7.3 Support Agreements

To provide best value and consistent pricing, the services described within this document assume that existing customer software/provider/manufacturer support or warranty agreements will remain in-place and be accessible by Roc to facilitate a swift response to any security issues raised around third-party offerings.

2.7.4 Service & Operational Tooling

Roc can provide access to our own service and operational management tools or leverage clients existing tool sets. Roc will require appropriate remote access and licences where client tools are leveraged.

2.7.5 Change Management

It is assumed that each in-scope supported item will be fully managed by Roc, in line with the agreed change management process. Whilst the client and other 3rd parties chosen by them can retain administrative access (e.g. for emergency/auditing purposes), it is assumed that all changes to an in-scope supported item will be performed by Roc.

One hour of change management time per month is included for each in-scope supported Item. This will be fulfilled during normal business hours. Additional service points can be purchased as required for the fulfilment of additional services.

2.8 Service Level Agreements

The below table summarises the SLAs offered as part of Roc Managed Cloud Services.

2.8.1 Hours of Cover

Roc's Managed Cloud Services are offered based upon two standard SLA's:

- Normal Business Hours: Monday to Friday, 08:00-18:00, excluding public holidays
- 24x7: 24 hours per day, 7 days per week, 365 days per year

2.8.2 Incident Management

PRIORITY	DEFINITION	TARGET RESPONSE	TARGET UPDATE	TARGET RESOLUTION
P1 (Critical)	Critical Business Impact. A complete service failure or severe degradation of service. Typically impacting >50% of users at a supported site, or >50% users of a	30m	1h	4h

	supported system. No acceptable workaround available. Examples include: - • Complete network failure • Simultaneous failure of resilient WAN links • Core application/service down			
P2 (Serious)	Serious business impact. A widespread degradation of service, typically impacting all or a significant number (>25%) of users at a supported site, or of a supported system. Examples include: • Severe network performance degradation • Severe application performance degradation • Failure of non-resilient WAN links • Extended application functionality failure for all users • A loss of system resiliency	30m	1h	8h
P3 (Medium)	Medium business impact, A partial or intermittent degradation of service. Typically impacting a subset, group, or individual system users. Examples include: • Partial/intermittent network degradation • Partial/intermittent application degradation • System failure impacting individuals • Extended application functionality failure	2h	10h	16h
P4 (Low)	Low/minimal business impact. Typically, non-critical loss of service/functionality, or minor degradation of service for individual users. Examples include: • Network issues affecting lab/test Equipment • Applications issues when testing changes • Partial application degradation for individuals • Threshold breeches with no impact on service.	10h	20h	40h

2.8.3 Change Management

DEFINITION	TARGET SLA
'Standard' Change Request List to be agreed during service initiation and regularly reviewed/updated during service operation	5 Days - to complete
'Non-Standard' Change Request*	10 Days - to complete.

2.8.4 SLA Terms

1. The SLA times within the above tables are offered as a target time against which Roc's performance will be assessed.
2. The SLA clocks will run during the agreed hours of cover. Where 24x7 cover has been purchased the SLA clock will run outside of normal hours for P1 & P2 incidents only
3. Where the priority of an incident cannot be agreed, the client's decision will apply. Should this occur frequently, it will be addressed during the service review meetings.
4. All incident requests will be logged within the agreed service management toolset. A minimum data set will be mutually agreed for a request to be logged. An incident request will be considered as 'logged' once the clients service desk has documented the minimum dataset and assigned the request to Roc's resolver group.
5. The 'Response' SLA is measured from the time at which an incident is 'logged' to the time at which its status changes to 'Work in Progress', typically because: Remote investigation has commenced.
6. The 'Resolution' SLA is measured from the time at which an incident is 'logged' to the time at which its status changes to 'resolved'.
7. Incident 'Updates' will be provided via ticket updates, phone, voicemail, email or in-person dialogue with customer contacts.
    - SLA clocks will be paused if a request cannot reasonably be progressed for reasons outside of Roc's control.
    - Awaiting further information from the client and thus no progression is possible.
    - Awaiting onsite engineering support.
    - Awaiting testing confirmation from the user/requestor.
    - Awaiting client approval for additional costs.
    - Awaiting a third party or manufacturer action which is outside of Roc's direct control.
    - Awaiting the completion/approval of a relevant change request.
8. The incident SLA clocks will also be paused if an acceptable work around is implemented, and the priority level reduced.
9. Roc will require the ability/authority to liaise directly with any in-scope software vendors, manufactures of service providers, to obtain software updates or TAC support.
10. A Major Incident Report (MIR) will be provided within 5 working days for any P1 or P2 incident which exceeds the committed SLA's, exhibits a process failure or where there is a clear opportunity for service improvement.
11. During the service provision, systems will be maintained at supported software versions and in line with manufacturer best practice. From time-to-time Roc may also make recommendations to improve the security, performance, or availability of an in-scope item.

2.8.5 Service Delivery Management

Roc provides two standard packages of service delivery management 'Standard' and 'Enhanced':

PACKAGE	DESCRIPTION
Standard	• Standard Roc Service Report Template. • Quarterly service review performed remotely.
Enhanced	• Customised/Bespoke service report template • Monthly or quarterly service reviews performed remotely. • Quarterly onsite service reviews with aligned SDM. • Tailored observations & recommendations. • Continual Service Improvement Plan (CSIP).

Roc will incorporate standard service reporting within the scope of a Managed Service. The service reports will cover the following:

- A summary of all incidents and service requests logged with the Service Desk.
- A list of outstanding incidents and service requests and their status.
- Roc's performance against the service levels in the relevant month.
- Updates to agreed MIR remedial actions.
- 3rd party performance against their committed service levels.
- Quantitative and qualitative service reports/graphs.
- Infrastructure reports with relevant information on capacity, performance, and availability.
- Support advisories (for example end-of-life statement and upgrade recommendations).
- Software advisories (for example recommended updates).
- General observations and recommendations.

2.8.6 Continuous Improvement

Roc places high value on the delivery of Continuous Service Improvement (CSI) and Customer Experience to drive business value and efficiency. CSI will be driven by Service Delivery Manager and Account Manager. Each service improvement item will define the business outcomes and be driven by key metrics around customer value and experience.

We would continually monitor SLA and KPI performance throughout the contract term and provide reporting through Service Reviews. In terms of contractual remedies, the key premise is this should be measured against SLA and KPI performance.

3. Service Pricing

Refer to Roc's pricing document representing Additional Service Points

3.1 Onboarding Fees

For each new service provision, a one-time on-boarding charge will apply. This fee is charged to cover transition activity such as process definition, toolset configuration, system discovery, remote access configuration and knowledge management tasks. This charged will be in line with Roc's published SFIA Rate card and will vary based upon the nature and complexity of the environment to be on-boarded.

During the on-boarding process, Roc will review the configuration of each in-scope item. Where in-scope items have not been configured in-line with best practice, remedial actions may be required before the item can be on-boarded or covered by Roc's SLA's. Such remedial activity can be performed by the client or Roc. Where performed by Roc it can be funded via Roc's published SFIA Rate card or the Additional Service Points purchased as part of the service.

Roc follows a mature service transition process for on-boarding new Managed Services:

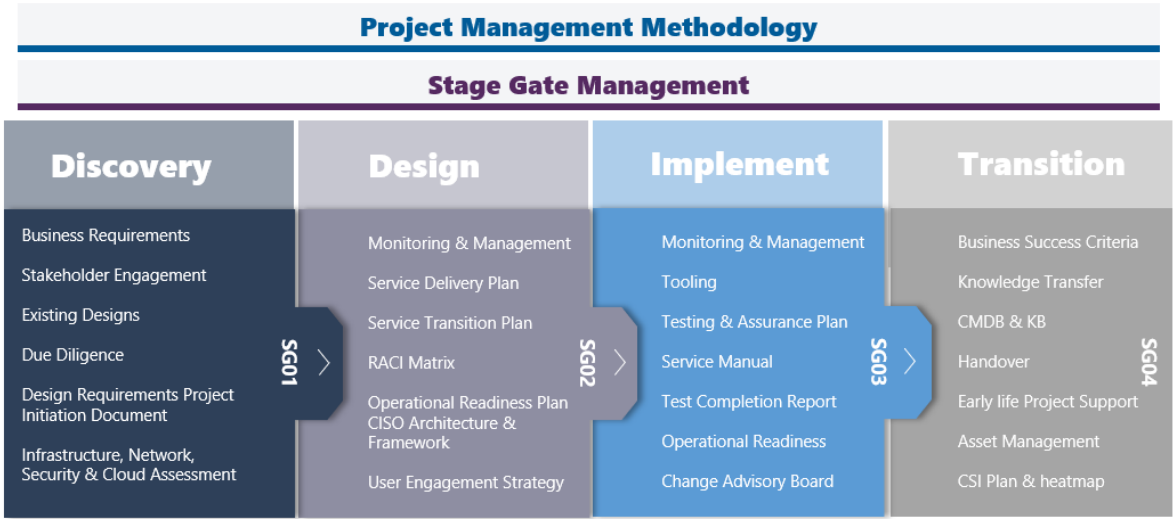

Figure 6 – Roc Service Transition Process

4. Terms and Conditions

Refer to Roc's Terms and conditions documents included with the submission. Standard terms are relevant to smaller one-off purchases, and the Master Service Agreement (MSA) is applicable for longer term contracts.